ON THE APPLICATIONS OF CYCLOTOMIC FIELDS IN INTRODUCTORY NUMBER THEORY

KABALAN GASPARD

Abstract. In this essay, we see how prime cyclotomic fields (cyclotomic fields obtained by adjoining a primitive p-th root of unity to $\mathbb{Q}$, where p is an odd prime) can lead to elegant proofs of number theoretical concepts. We namely develop the notion of primary units in a cyclotomic field, demonstrate their equivalence to real units in this case, and show how this leads to a proof of a special case of Fermat's Last Theorem. We finally modernize Dirichlet's solution to Pell's Equation.

Throughout this paper, unless specified otherwise, $\zeta \equiv \zeta_p \equiv e^{\frac{2\pi\sqrt{-1}}{p}}$ where p is an odd prime. $K \equiv \mathbb{Q}(\zeta)$ and $\mathcal{O}_K$ is the ring of integers of K. We assume knowledge of the basic properties of prime cyclotomic fields that can be found in any introductory algebraic number theory textbook, namely that:

- $Gal(K : \mathbb{Q}) \simeq U(\mathbb{Z}/p\mathbb{Z})$ (the group of units of $\mathbb{Z}/p\mathbb{Z}$), which is cyclic and of order $p-1$.
- $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \left\langle 1, \zeta_p, ..., \zeta_p^{p-2} \right\rangle_{\mathbb{Z}}$, where $\left\{1, \zeta_p, ..., \zeta_p^{p-2}\right\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$.
- The only roots of unity in $\mathcal{O}_K$ (i.e. solutions in $\mathbb{C}$ to $x^n = 1$ for some $n \in \mathbb{N}$) are of the form $\pm\zeta_p^i$, $i \in \mathbb{Z}$.

We also assume elementary knowledge of quadratic characters, quadratic reciprocity, and the Legendre symbol $\left(\frac{k}{p}\right)$.

1. Primary elements in $\mathcal{O}_K$

Definition 1. *Let $\alpha \in \mathcal{O}_K$ with α prime to p. Then α is* primary *iff α is congruent to a rational integer modulo $(1-\zeta_p)^2$.*

Date: June 22, 2011, re-edited February 11, 2012.

The definition of primary elements has historically been ambiguous in Number Theory. In [2], Dalawat shows that definitions of primary elements in $\mathcal{O}_K$ even differ by country ("p-primary", "*primaire*" and "*primär*") and, even though these definitions do form a chain of implications, they are not equivalent.

We also note that it is not true that if p an arbitrary odd prime and μ prime in $\mathcal{O}_K$, only one associate of μ is primary (for example, according to the above definition, both $\pm(4+3\omega)$ are primary in the ring of integers of $\mathbb{Q}(\omega)$ where $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$).

Proposition 1. *Let $\alpha \in \mathcal{O}_K$ (not necessarily prime) and suppose α prime to p in $\mathcal{O}_K$. Then there exists a $k \in \mathbb{Z}$, unique (modulo p), such that $\zeta_p^k \alpha$ is primary.*

Proof. Consider the ideal $P = (1-\zeta_p)$ in $\mathcal{O}_K$. Then the norm of the ideal $N(P) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = p$ by the fact that $Gal(K:\mathbb{Q}) \simeq U(\mathbb{Z}/p\mathbb{Z})$. So P is a prime ideal and is thus of degree 1. So by Dedekind's Theorem in Algebraic Number Theory, any element of $\mathcal{O}_K$ is the root of a monic polynomial of degree 1 in $\mathcal{O}_K/P$. So in the particular case of α, $\alpha - a_0 = \overline{0}$ in $\mathcal{O}_K/P$ for some $a_0 \in \mathbb{Z}$. In other words, $\alpha \equiv a_0\ (1-\zeta_p)$. So $\frac{\alpha - a_0}{(1-\zeta_p)} \in \mathcal{O}_K$ and so, by the same argument, $\frac{\alpha-a_0}{(1-\zeta_p)} \equiv a_1\ (1-\zeta_p)$ for some $a_1 \in \mathbb{Z}$. We stop repeating this here because multiplying the congruence by $(1-\zeta_p)$, we now have a congruence modulo $(1-\zeta_p)^2$, which is what we want to consider. More precisely, we now have $\alpha - a_0 \equiv a_1(1-\zeta_p)\ \ (1-\zeta_p)^2$, so $\alpha \equiv a_0 + a_1(1-\zeta_p)\ \ (1-\zeta_p)^2$.

We want to eliminate the $(1-\zeta_p)$ term by multiplying both sides by ζ_p^n for some $n \in \mathbb{Z}$. Notice that $\zeta_p = (1-(1-\zeta_p))$. So modulo $(1-\zeta_p)^2$,

$$\begin{aligned}
\zeta_p^n \alpha &\equiv \zeta_p^n a_0 + a_1 \zeta_p^n (1-\zeta_p) \\
&\equiv a_0(1-(1-\zeta_p))^n + a_1(1-\zeta_p)(1-(1-\zeta_p))^n \\
&\equiv a_0(1-n(1-\zeta_p)) + a_1(1-\zeta_p)(1-n(1-\zeta_p))
\end{aligned}$$

since considering $(1-(1-\zeta_p))^n$ as a polynomial in $(1-\zeta_p)$, $(1-\zeta_p)^2$ divides $(1-\zeta_p)^i$ for $i \geq 2$. So

$$\zeta_p^n \alpha \equiv a_0 + (a_1 - n a_0)(1-\zeta_p) \quad (1-\zeta_p)^2$$

Now α prime to p, so if $a_0 \equiv 0\ (p)$, then $a_0 \equiv 0\ (1-\zeta_p)$, and so $\alpha \equiv 0\ (1-\zeta_p)$, which is a contradiction. So $a_0 \not\equiv 0\ (p)$, and so $a_1 - na_0 \equiv 0$ has a **unique** solution k modulo p. Now $(1-\zeta_p) \mid (1-\zeta_p^2)$, and $N(\frac{1-\zeta_p^2}{1-\zeta_p}) = \frac{N(1-\zeta_p^2)}{N(1-\zeta_p)} = 1$, so $(1-\zeta_p^2)$ is associate to $(1-\zeta_p)$. It follows that $(1-\zeta_p)^2 \mid p$, and so k is (still, since $a_1 - na_0 \in \mathbb{Z}$) the **unique** integral solution modulo p to $a_1 - na_0 \equiv 0\ \ (1-\zeta_p)^2$. Then $\zeta_p^k\alpha \equiv a_0\ (1-\zeta_p)^2$, and therefore $\zeta_p^k\alpha$ is primary. □

Lemma 1. *Let u be a unit in $\mathcal{O}_K$. Then $\frac{u}{\overline{u}} = \zeta^t$ for some $t \in \mathbb{Z}$*

Proof. Write $\upsilon = \frac{u}{\overline{u}}$. Conjugation is a Galois automorphism on $\mathcal{O}_K$ since $\overline{\zeta} = \zeta^{-1} = \zeta^{p-1}$. So $\overline{u}$ is also a unit, and so $\upsilon \in \mathcal{O}_K$. Now let σ_k be the $(p-1)$ Galois automorphisms on $\mathcal{O}_K$ such that $\sigma_k(\zeta) = \zeta^k$, $k \in \mathbb{Z}$. Then for all $1 \le k \le (p-1)$, $\sigma_k\upsilon = \frac{\sigma_k u}{\sigma_k\overline{u}} = \frac{\sigma_k u}{\overline{\sigma_k u}}$ by the above remark. So $|\sigma_k\upsilon| = \sigma_k\upsilon\overline{\sigma_k\upsilon} = 1$. So $|\sigma_k\upsilon|^n = 1$ for any $n \in \mathbb{N}$.

Now consider the polynomial $f(x) = \prod_{k=1}^{p-1}(x - \sigma_k\upsilon)$. The coefficients of this polynomial are elementary symmetric polynomials in $\{\sigma_k\upsilon : 1 \le k \le p-1\}$, and so are invariant by action by $Gal(K:Q) = \{\sigma_k\upsilon : 1 \le k \le p-1\}$. So $f(x) \in \mathbb{Z}[x]$. But then the coefficient of x^k is $s_{(p-1)-k}$ where s_j is the j^{th} elementary symmetric polynomial. But by the previous paragraph, $\left|s_{(p-1)-k}\right| \le \sum_{j=1}^{p-1-k} |\sigma_k\upsilon|^k \le p-1-k$. So there are finitely many possible such $f(x) \in \mathbb{Z}[x]$ since the coefficients are bounded. So there are finitely many possible roots since a polynomial of finite degree has a finite number of roots. But $|\sigma_k\upsilon^n| = 1$ for any $n \in \mathbb{N}$, so $\{\upsilon^n : n \in \mathbb{N}\}$ satisfy the same argument. So we must have $\upsilon^n = \upsilon^{n'}$ for some $n, n' \in \mathbb{Z}$. So $\upsilon^{n-n'} = 1$, and it follows that υ is a root of unity in $\mathcal{O}_K$.

So by the basic properties of prime cyclotomic fields, we must have $\upsilon = \pm\zeta^t$ for some $t \in \mathbb{Z}$. Now consider congruence modulo $\lambda = 1-\zeta$. Then since $\frac{1-\zeta^k}{1-\zeta} = \sum_{i=1}^{k-1}\zeta^i \in \left\langle 1, \zeta_p, ..., \zeta_p^{p-2}\right\rangle_{\mathbb{Z}} = \mathcal{O}_K$, $\zeta^k \equiv 1\ (\lambda)$ for all $k \in \mathbb{Z}$. So since $\overline{\zeta^k} = \zeta^{-k} \equiv 1 \equiv \zeta^k\ (\lambda)$, $\alpha \equiv \overline{\alpha}\ (\lambda)$ for all $\alpha \in \mathcal{O}_K$. Namely, $u \equiv \overline{u} = \pm\zeta^{-t}u \equiv \pm u\ (\lambda)$. So if $\upsilon = -\zeta^t$, $u \equiv -u\ (\lambda) \Rightarrow 2u \equiv 0\ (\lambda)$ which is impossible since $N(\lambda) = p \nmid N(2u) = 2^{p-1}$ since p is odd. So $\upsilon = +\zeta^t$. □

Theorem 1. *Let u be a unit in $\mathcal{O}_K$. Then u is real $\Leftrightarrow$ u is primary in $\mathcal{O}_K$.*

Proof. Since $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \left\langle 1, \zeta_p, ..., \zeta_p^{p-2}\right\rangle_{\mathbb{Z}}$, we can write u as $\sum_{k=0}^{p-2} a_k\zeta^k$ for unique $a_0, ..., a_{p-2} \in \mathbb{Z}$. And so, noting that $\zeta^{p-1} = -\sum_{i=0}^{p-2}\zeta^i$, $\zeta^{-t}u = \sum_{k=0}^{p-2} a_k\zeta^{k-t} = \sum_{k=0}^{p-2}(a_{k+t} - a_{(p-1)+t})\zeta^k$ where

a_k is defined to be $a_{(k \bmod p)}$ for all $k \notin \{0, ..., p-1\}$ ($a_{p-1} = 0$, trivially). And so $\sum_{k=0}^{p-2}(a_{p-k} - a_1)\zeta^k = \overline{u} = \zeta^{-t}u = \sum_{k=0}^{p-2}(a_{k+t} - a_{(p-1)+t})\zeta^k$ by 1 and therefore, since this representation is unique, we get

$$a_{k+t} - a_{(p-1)+t} = a_{p-k} - a_1 \text{ for all } 0 \leq k \leq p-1 \tag{1.1}$$

Letting k_0 be the $\bmod p$ solution to $k + t \equiv p - k\ (p)$, we get $a_{k_0+t} = a_{p-k_0}$ and so (1.1) yields $a_{(p-1)+t} = a_1$. (1.1) then becomes

$$a_{k+t} = a_{p-k} = a_{-k} \text{ for all } 0 \leq k \leq p-1 \tag{1.2}$$

Since replacing k by $-(k+t)$ in (1.2) leaves the equation invariant, we get $\frac{p-1}{2}$ pairs of equal terms with distinct indices amongst $a_0, ..., a_{p-1}$ (the 'remaining' term being a_{k_0+t}). Let $b_1, ..., b_{\frac{p-1}{2}}$ be representatives of these distinct pairs, and let $b_{k_0+t} = a_{k_0+t}$ (we have simply selected and reordered the a_i's).

Now by the proof of 1, there is a unique c modulo p such that $\zeta^c u$ is primary, and this c is the solution to $ax \equiv b\ (p)$ where $u \equiv a + b\lambda\ (\lambda^2)$ where $\lambda = (1 - \zeta)$. Now $u = \sum_{k=0}^{p-2} a_k \zeta^k$. Writing, as a polynomial, $f(x) = \sum_{k=0}^{p-2} a_k x^k$, we can find a and b by finding the coefficients of 1 and x respectively of $f(1-x)$ since $\zeta = 1 - \lambda$. Making elementary use of the Binomial Theorem, we see that $f(1-x) = \sum_{k=0}^{p-2} a_k (1-x)^k = \sum_{k=0}^{p-2} a_k - \sum_{k=0}^{p-2} k a_k x + ...$ (we only need the first two terms). So c is the solution to

$$\left(\sum_{k=0}^{p-2} a_k\right) x \equiv -\sum_{k=0}^{p-2} k a_k\ (p) \tag{1.3}$$

Which, since $a_{p-1} = 0$, is equivalent to

$$\left(\sum_{k=0}^{p-1} a_k\right) x \equiv -\sum_{k=0}^{p-1} k a_k\ (p) \tag{1.4}$$

Now $k_0 + t \equiv p - k_0\ (p) \Rightarrow k_0 + t \equiv -(k_0 + t) + t\ (p) \Rightarrow (k_0 + t) \equiv 2^{-1}t \Rightarrow b_{k_0+t} = a_{k_0+t} = a_{2^{-1}t}$. Finally, note that for $a_i = a_{t-i} = b_l$ for $1 \leq l \leq \frac{p-1}{2}$ by (1.2), $ia_i + (t-i)a_{t-i} = tb_l$.

(1.4) then becomes $\left(b_{k_0+t} + 2\sum_{k=1}^{\frac{p-1}{2}} b_k\right) x \equiv -\left((2^{-1}t \bmod p)b_{k_0} + \sum_{k=1}^{\frac{p-2}{2}} tb_k\right)$ (p). It is clear that $c \equiv -2^{-1}t$ (p) is the solution to this congruence. By its uniqueness, we see that u is primary $\Leftrightarrow t \equiv 0$ $(p) \Leftrightarrow u = \zeta^t\overline{u}$ is real. □

2. Application to a Special Case of Fermat's Last Theorem

Fermat's well-known final theorem, proved by Andrew Wiles and Richard Taylor in 1994, states that

$$x^n + y^n = z^n$$

where $x, y, z, n \in \mathbb{Z}$ has no non-trivial solutions (x, y, z) for $n \geq 3$.

In fact, to prove this theorem, it suffices to prove that $x^p + y^p = z^p$ has no integral solutions for any positive odd prime p, since $x_0^n + y_0^n = z_0^n \Rightarrow x_1^p + y_1^p = z_1^p$ where p is an odd prime dividing n (exists since $n \geq 3$) and $(x_1, y_1, z_1) = (x_0^{n/p}, y_0^{n/p}, z_0^{n/p})$. In other words, we can restrict our study to the case where n is an odd prime.

There is a very elegant proof of a special case of this theorem using cyclotomy. The main use of the concept here is that it allows us to transform a "sum of n-th powers" problem into a "divisibility" problem since we can now factor $x^p + y^p$ as $\prod_{i=0}^{p-1}(x + \zeta_p^i y)$.

In this section, we shall lay out said proof. Let $K = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_p$. We will suppose that for some (x_0, y_0, z_0) is a solution to $x^p + y^p = z^p$ for some odd prime p. Then

$$x_0^p + y_0^p = z_0^p \tag{2.1}$$

WLOG, we can take x_0, y_0 and z_0 to be pairwise relatively prime, for if some $d \in \mathbb{Z}$ divides two of them, it must divide the 3rd, and then $x_0^p + y_0^p = z_0^p \Leftrightarrow x_1^p + y_1^p = z_1^p$ where $x_0, y_0, z_0 = dx_1, dy_1, dz_1$ respectively, with $x_1, y_1, z_1 \in \mathbb{Z}$.

We shall now reduce the problem to a special case and suppose that *p does not divide the class number h of O_K*, and that $p \nmid x_0y_0z_0$. From (2.1), we shall reach a contradiction.

This case has been treated in Number Theory textbooks such as [1]. However, using the

equivalence of primary and real units in $\mathcal{O}_K$ when K is a prime cyclotomic field, we can prove the result more rapidly.

Lemma 2. *Let $i \not\equiv j$ (p). Then the ideals $I = (x_0 + \zeta^i y_0)$ and $J = (x_0 + \zeta^j y_0)$ are relatively prime.*

Proof. Consider the ideal $I+J$. J contains the element $-(x_0+\zeta^j y_0)$, so $x_0+\zeta^i y_0-(x_0+\zeta^j y_0) = (\zeta^i - \zeta^j)y_0 \in I + J$. Likewise, since $\mathcal{O}_K = \mathbb{Z}[\zeta]$, $-\zeta^j(x_0 + \zeta^i y_0) = \zeta^j x_0 + \zeta^{i+j} y_0 \in I$ and $\zeta^i(x_0 + \zeta^j y_0) = \zeta^i x_0 + \zeta^{i+j} y_0 \in J$. So $\zeta^i x_0 + \zeta^{i+j} y_0 - \zeta^j(x_0 + \zeta^i y_0) = (\zeta^i - \zeta^j)x_0 \in I + J$. Now $(x_0, y_0) = 1 \Rightarrow$ there exist $a, b \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$. So $a(\zeta^i - \zeta^j)x_0 + b(\zeta^i - \zeta^j)y_0 = (\zeta^i - \zeta^j) \in I + J$.

Now $N(\zeta^i - \zeta^j) = p$ since $(N(\zeta^i - \zeta^j))^2 = \prod_{k=1}^{p-1}(\zeta^{ik} - \zeta^{jk})^2 = \prod_{k=1}^{p-1}(-\zeta^{-k(j-i)})(1 - \zeta^{k(j-i)})^2 = \prod_{k=1}^{p-1}(-\zeta^{-k})(1 - \zeta^k)^2 = +\zeta^{-p\frac{p-1}{2}} \prod_{k=1}^{p-1}(1 - \zeta^k)^2 = 1 \cdot \left(\sum_{k=1}^{p-1} 1\right)^2 = p^2$. So $N(I + J) \mid p$. If $N(I + J) = p$, then since $I \subseteq I + J$, $p = N(I + J) \mid N(I) = \prod_{i=0}^{p-1}(x_0 + \zeta^i y_0) = x_0^p + y_0^p = z_0^p$. So since p is prime, $p \mid z_0 \Rightarrow$ contradiction. So $N(I + J) = 1$, and therefore $I + J = \mathcal{O}_K$. So I and J are coprime since $P \mid I$ and $P \mid J \Rightarrow P \mid I + J \Rightarrow P = \mathcal{O}_K$. □

Now $x_0^p + y_0^p = z_0^p \Rightarrow \prod_{i=0}^{p-1}(x_0 + \zeta^i y_0) = (z_0)^p$ as ideals. But $\{(x_0 + \zeta^i y_0) : 0 \leq i \leq p-1\}$ are pairwise coprime. So by unique factorization of ideals, each of these ideals must be a p-th power. So in particular, taking $i = 1$, $(x_0 + \zeta y_0) = \mathfrak{I}^p$ for some ideal $\mathfrak{I}$. So since $(x_0 + \zeta y_0)$ is principal, $[\mathfrak{I}]$ has order dividing p in the ideal class group, but since $p \nmid h$, we must have that the order of $[\mathfrak{I}]$ is 1. So $\mathfrak{I}$ is principal. Let $\mathfrak{I} = (\alpha)$. Then $(x_0 + \zeta y_0) = (\alpha^p)$, and so $x_0 + \zeta y_0$ is associate to α^p. We write $x_0 + \zeta y_0 = u\alpha^p$ where u is a unit in $\mathcal{O}_K$.

Then by 1 there exists a unique c modulo p such that $\zeta^{-c}u$ is primary. Let $\zeta^{-c}u = u_0$ so that $u = \zeta^c u_0$ where u_0 is primary. But u_0 is trivially a unit, and is therefore real by 1.

So $x_0+\zeta y_0 = \zeta^c u_0 \alpha^p$ where u_0 is real. Note that modulo p, $\alpha^p \equiv \left(\sum_{i=0}^{p-2} a_i \zeta^i\right)^p \equiv \sum_{i=0}^{p-2} a_i^p \zeta^{ip} \equiv \sum_{i=0}^{p-2} a_i^p \in \mathbb{Z}$ (p). So $\alpha^p \equiv \overline{\alpha^p}$ (p). It follows that $x_0 + \zeta y_0 = \zeta^c u_0 \alpha^p \Rightarrow x_0 + \zeta y_0 \equiv \zeta^c u_0 \alpha^p$ $(p) \Rightarrow \overline{x_0 + \zeta y_0} \equiv \overline{\zeta^c u_0 \alpha^p}$ $(p) \Rightarrow x_0 + \zeta^{-1} y_0 \equiv \zeta^{-c} u_0 \alpha^p$ (p). So we now have $x_0 + \zeta y_0 \equiv \zeta^c u_0 \alpha^p$ $(p) \Rightarrow \zeta^{-c} x_0 + \zeta^{1-c} y_0 \equiv u_0 \alpha^p$ (p) and $x_0 + \zeta^{-1} y_0 \equiv \zeta^{-c} u_0 \alpha^p$ $(p) \Rightarrow \zeta^c x_0 + \zeta^{c-1} y_0 \equiv u_0 \alpha^p$ (p).

Subtracting the latter congruence from the former yields

$$\zeta^{-c}x_0 + \zeta^{1-c}y_0 - \zeta^c x_0 - \zeta^{c-1}y_0 \equiv 0 \ (p) \tag{2.2}$$

Now an element of $\mathcal{O}_K = \mathbb{Z}[\zeta]$ is divisible by p if and only if all of the coefficients as a polynomial in ζ are divisible by p. $p \nmid x_0, y_0$ since $p \nmid x_0 y_0 z_0$, so we must check the cases where one of $\{c, -c, 1-c, c-1\}$ is congruent to -1 modulo p or where two of $\{c, -c, 1-c, c-1\}$ are equal modulo p. These cases can be split as follows:

- $c \equiv 0 \ (p)$ (so that $c \equiv -c \ (p)$). Then $p \mid y_0(\zeta - \zeta^{-1}) = y_0(\sum_{i=2}^{p-2} \zeta^i + 1) \Rightarrow p \mid y_0$ (even if $p = 3$) $\Rightarrow$ contradiction.
- $c \equiv 1 \ (p)$ (so that $1 - c \equiv c - 1 \ (p)$). Then $p \mid x_0(\zeta^{-1} - \zeta) \Rightarrow p \mid x_0$ as in the previous case $\Rightarrow$ contradiction.
- $c \equiv 2^{-1} \ (p)$ (so that $c \equiv 1 - c \ (p)$). Then $p \mid (y_0 - x_0)\zeta^c + \zeta^{-c}(x_0 - y_0)$. So $p \mid (x_0 - y_0)$. We then rewrite 2.1 as $x_0^p + (-z_0)^p = (-y_0)^p$ (since p is odd). Then with the same argument we will get $p \mid (x_0 + z_0)$. But 2.1 yields $x_0^p + y_0^p - z_0^p \equiv 0 \ (p)$ and so $x_0 + y_0 - z_0 \equiv 0 \ (p)$. This yields $3x_0 \equiv 0 \ (p)$. We suppose for now that $p > 3$. Then this yields $p \mid x_0 \Rightarrow$ contradiction.
- Letting one of $\{c, -c, 1-c, c-1\}$ be congruent to -1 modulo p will yield one of the coefficients of the terms of (2.2) as $\pm(x_0 - y_0)$, giving the same contradiction as in the previous case.

We therefore obtain a contradiction in all cases. We have, however, supposed that $p > 3$. A general study of the case where $p = 3$ is done elegantly in [4].

3. An Approach to Pell's Equation using cyclotomy

Pell's Equation is

$$x^2 - dy^2 = 1, \quad x, y \in \mathbb{Z}$$

in x and y, where $d \in \mathbb{Z}^+$. $d \leq 0$ trivially yields the single solution $(1, 0)$, and we can consider d to be square-free, since any square factor of d can be incorporated into y.

The equation can be solved using cyclotomy and quadratic residues. A partial solution was found by Dirichlet using this method, building upon the work of Gauss [3]. In this section, we build upon Dirichlet's work, explicitly writing the solution and using the modern machinery of Galois Theory to streamline the approach. Again, we let p be an odd prime, and define $p^* = (-1)^{\frac{p-1}{2}}p$, $i = \sqrt{-1}$, and start by introducing an important lemma.

Lemma 3. $\begin{cases} q_1(x) = 2\prod\limits_{\substack{1\le k<p \\ \left(\frac{k}{p}\right)=1}} (x-\zeta^k) = f(x) + \sqrt{p^*}g(x) \\ q_{-1}(x) = 2\prod\limits_{\substack{1\le k<p \\ \left(\frac{k}{p}\right)=-1}} (x-\zeta^k) = f(x) - \sqrt{p^*}g(x) \end{cases}$ *where $f(x), g(x)$ are polynomials in $\mathbb{Z}[x]$.*

Proof. Note that the product of the 2 above polynomials (on the left-hand side) is $4\prod\limits_{1\le k<p}(x-\zeta^k) = 4m_p(x) \in \mathbb{Z}[x]$. It is therefore fixed by any Galois automorphism in $Gal(K:\mathbb{Q})$. Now taking $\theta = \zeta^{\frac{p^2-1}{8}}\prod\limits_{k=1}^{\frac{p-1}{2}}(1-\zeta^k)^2$, we see that $\theta^2 = p^*$ since $(-1)^{\frac{p^2-1}{8}} \equiv \left(\frac{2}{p}\right) \pmod 2$, and trivially $\theta \in \mathcal{O}_K$. So $\sqrt{p^*} \in \mathcal{O}_K$, Now an automorphism σ in the Galois group fixes p^* if and only if σ is a square. But this is if and only if σ fixes all (and only) the ζ^k such that k is a quadratic residue modulo p. So $\prod\limits_{\substack{1\le k<p \\ \left(\frac{k}{p}\right)=1}} (x-\zeta^k) \in L[x]$ where $L = \mathbb{Q}(\sqrt{p^*})$. All the coefficients in $L[x]$ are of the form $a + b\sqrt{p^*}$ where a and b are both rational, and $\frac{1}{2}\cdot$ an algebraic integer (allowing for the fact that $p^* \equiv 1\ (4)$). The coefficients of $2\prod\limits_{\substack{1\le k<p \\ \left(\frac{k}{p}\right)=1}} (x-\zeta^k)$ are therefore rational algebraic integers and thus in $\mathbb{Z}$. We can now expand $q_1(x)$ and rewrite it as $q_1(x) = f(x) + \sqrt{p^*}g(x)$ where $f(x), g(x)$ are polynomials in $\mathbb{Z}[x]$.

A similar argument shows that $q_{-1}(x) \in L[x]$. Now let τ be the Galois automorphism in $Gal(K:Q)$ defined by $\tau(\sqrt{p^*}) = -\sqrt{p^*}$ (noting that $K:L:\mathbb{Q}$ is a tower of fields). Then by the above, and since τ^2 must fix $q_1(x)$, we must have that $\tau(\zeta^k) = \zeta^l$ where $\left(\frac{k}{p}\right)\left(\frac{l}{p}\right) = -1$. So since τ is a Galois automorphism over K, we must have $\tau(q_1(x)) = q_{-1}(x)$. This yields that $q_{-1}(x) = f(x) - \sqrt{p^*}g(x)$. □

We will primarily consider the case where d is an odd prime. Pell's Equation then becomes

$$x^2 - py^2 = 1 \tag{3.1}$$

By Lemma 3,

$$4m_p(x) = q_1(x)q_{-1}(x) = f(x)^2 - (p^*)g(x)^2$$

And so, replacing x by 1, we get

$$4p = x_1^2 - p^* y_1^2 \text{ where } x_1 = f(1),\ y_1 = g(1) \tag{3.2}$$

Since $f(x), g(x) \in \mathbb{Z}[x]$, $x_1, y_1 \in \mathbb{Z}$, and we can see that Lemma 3 relates to Pell's Equation insofar as it gives us a pair (x_1, y_1) that verifies an equation very similar to (3.1).

$4p = x_1^2 - p^* y_1^2 \Rightarrow x_1^2 = 4p + p^* y_1^2 \Rightarrow p \mid x_1^2 \Rightarrow p \mid x_1$ since p is prime. So letting $p\xi_1 = x_1$, we can rewrite equation (3.2) as $4p = p^2\xi_1^2 - p^* y_1^2$, and so, dividing by p,

$$p\xi_1^2 - (-1)^{\frac{p-1}{2}} y_1^2 = 4 \tag{3.3}$$

We now analyze $q_1(x)$ and $q_{-1}(x)$ to obtain some insight as to the values x_1 and y_1. $x^2 \equiv (p-x)^2\ (p)$, so all quadratic residues are in $\{x^2\ (p) : 1 \leq x \leq \frac{p-1}{2}\}$. We can therefore reorder the terms in $q_1(x)$ and write it as $2\prod_{k=1}^{\frac{p-1}{2}}(x - \zeta^{k^2})$, and so $q_1(1) = 2\prod_{k=1}^{\frac{p-1}{2}}(1 - \zeta^{k^2})$.

The value of p^* depends on the value of p modulo 4 so we will consider the two cases separately for simplicity.

Case 1: $p \equiv 1\ (4)$.

Then (3.3) becomes $p\xi_1^2 - y_1^2 = 4$ (or, to emphasize the similarity to Pell's Equation, $y_1^2 - p\xi_1^2 = -4$).

We then have two subcases.

If $p \equiv 1\ (8)$, then $y_1^2 - \xi_1^2 \equiv 4\ (8)$. Trivially y_1 and ξ_1 must either be both odd or both even. But $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1\ (8)$, so if y_1 and ξ_1 were both odd we would have $y_1^2 - \xi_1^2 \equiv 0\ (8) \Rightarrow$ contradiction. It follows that y_1 and ξ_1 are both even, and we can thus write $y_2 = \frac{y_1}{2}, \xi_2 = \frac{\xi_1}{2} \in \mathbb{Z}$. Then $y_2 - p\xi_2^2 = -1$. We can use the fact that $(\sqrt{p})^2 \in \mathbb{Z}$ to get rid of the minus sign in front of 1. $y_2^2 - p\xi_2^2 = -1$ yields $(y_2 - \sqrt{p}\xi_2)(y_2 + \sqrt{p}\xi_2) = -1$, and so $(y_2 - \sqrt{p}\xi_2)^2(y_2 + \sqrt{p}\xi_2)^2 = 1$. But $(y_2 \pm \sqrt{p}\xi_2)^2 = a \pm b\sqrt{p}$, $a, b \in \mathbb{Z}$. Taking $(x, y) = (a, b)$,

we have solved (3.1). Summarizing, we get a solution from

$$(a,b) = \left(\frac{1}{4}(g(1)^2+\frac{f(1)^2}{p}),\ \frac{f(1)g(1)}{2p}\right)$$
where we can directly compute $f(1)$ and $g(1)$

If $p\equiv 5\ (8)$, $y_1^2+3\xi_1^2\equiv 4\ (8)$. Given that the only quadratic residues modulo 8 are $0,1,4$, we must have $(y_1^2,\xi_1^2)\equiv(1,1),(0,4)$ or $(4,0)\ \ (8)$.

We now use the fact that $8^2=2^{2\cdot 3}=4^3$ and consider $(y_1+\sqrt{p}\xi_1)^3=(y_1^3+3p\xi_1^2y_1)+\sqrt{p}(p\xi_1^3+3y_1^2\xi_1)=y_2+\sqrt{p}\xi_2$ and see that $y_2^2-p\xi_2^2=(y_1^2-p\xi_1^2)^3=-4^3$.

But $y_2=y_1(y_1^2+3p\xi_1^2)\equiv y_1(y_1^2-\xi_1^2)\ (8)$. $(y_1^2,\xi_1^2)\equiv(1,1)\ (8)\Rightarrow y_2\equiv 0\ (8)$. $(y_1^2,\xi_1^2)\equiv(0,4)$ or $(4,0)\ (8)\Rightarrow y_2\equiv 4\cdot 4,\ 0\cdot 4$ or $\pm 2\cdot 4\equiv 0\ (8)$. So in any case $y_2\equiv 0\ (8)$.

Similarly $\xi_2=\xi_1(p\xi_1^2+3y_1^2)\equiv\xi_1(5\xi_1^2+3y_1^2)\ (8)$. $(y_1^2,\xi_1^2)\equiv(1,1)\ (8)\Rightarrow\xi_2\equiv\xi_2(5+3)\equiv 0$ (8). $(y_1^2,\xi_1^2)\equiv(0,4)$ or $(4,0)\ (8)\Rightarrow\xi_2\equiv\pm 2\cdot 4,\ 0\cdot 4$ or $4\cdot 0\equiv 0\ (8)$. So in any case $\xi_2\equiv 0$ (8).

So $8\mid y_2,\xi_2$ and thus, writing $y_3=\frac{y_2}{8},\xi_3=\frac{\xi_2}{8}\in\mathbb{Z}$, we get $(y_3^2-p\xi_3^2)=\frac{-4^3}{8^2}=-1$. As in the case where $p\equiv 1\ (8)$, writing $(y_3\pm\sqrt{p}\xi_3)^2=a\pm b\sqrt{p},\ a,b\in\mathbb{Z}$, $(x,y)=(a,b)$ is a solution of (3.1). Summarizing, we get a solution from

$$(a,b)=\begin{pmatrix}\frac{1}{64}((g(1)^3+\frac{3f(1)^2g(1)}{p})^2+p(\frac{f(1)^3}{p^2}+3\frac{g(1)^2f(1)}{p})^2)\ , \\ \frac{1}{32}(g(1)^3+3\frac{f(1)^2g(1)}{p})(\frac{f(1)^3}{p^2}+3\frac{g(1)^2f(1)}{p})\end{pmatrix}$$

Case 2: $p\equiv 3\ (4)$.

Let $l=\frac{p-1}{2}$. $p\equiv 3\ (4)\Rightarrow l$ is odd. We see that $f(x)=\frac{1}{2}(q_1(x)+q_{-1}(x))=\prod_{\substack{1\le k<p\\(\frac{k}{p})=1}}(x-\zeta^k)+$ $\prod_{\substack{1\le k<p\\(\frac{k}{p})=-1}}(x-\zeta^k)$. f is of degree l. We shall find a relation amongst the coefficients of f by comparing $f(\zeta)$ and $f(\overline{\zeta})=\overline{f(\zeta)}$ (since $f(x)\in\mathbb{Z}[x]$). Trivially $\left(\frac{1}{p}\right)=1$, so $\prod_{\substack{1\le k<p\\(\frac{k}{p})=1}}(\zeta-\zeta^k)=0$ and so $f(\zeta)=\prod_{\substack{1\le k<p\\(\frac{k}{p})=-1}}(\zeta-\zeta^k)$. Also note that $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=-1$, and so $\left(\frac{k}{p}\right)=-\left(\frac{-k}{p}\right)$ for all $1\le k\le p-1$. So $f(\zeta)=\prod_{\substack{1\le k<p\\(\frac{k}{p})=1}}(\zeta-\zeta^{-k})$. By the same line of reasoning, $f(\overline{\zeta})=f(\zeta^{-1})=$

$\prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} (\zeta^{-1}-\zeta^k)$. So

$$\begin{aligned}\frac{f(\zeta)}{f(\zeta^{-1})} &= \prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} \frac{(\zeta-\zeta^{-k})}{(\zeta^{-1}-\zeta^k)} = (-1)^l \prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} \zeta^{1-k}\\ &\quad \text{since there are precisely } l \text{ quadratic residues modulo } p\\ &= -\zeta^l \prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} \zeta^{-k}\\ &= -\zeta^l\\ &\quad \text{since } \sum_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} k = p\frac{p-1}{2}+0 \text{ since the Legendre symbol is a}\\ &\quad \text{quadratic character modulo } p \text{ and since } \left(\frac{0}{p}\right)=0.\end{aligned}$$

So $f(\zeta) = -\zeta^l f(\zeta^{-1})$. So writing $f(x) = a_l x^l + a_{l-1}x^{l-1} + ... + a_1 x + a_0$, this yields $a_l\zeta^l + a_{l-1}\zeta^{l-1} + ... + a_1\zeta + a_0 = -a_0\zeta^l - a_1\zeta^{l-1} - ... - a_{l-1}\zeta - a_l$, i.e.

$$\sum_{k=0}^{l} a_k\zeta^k = \sum_{k=0}^{l}(-a_k)\zeta^{l-k} \tag{3.4}$$

Now it is trivial to see that $a_l = 2$ by the above formula for $f(x)$. Also, $q_1(x) = 2\prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} (x-\zeta^k)$. The constant term of q_1 is $2(-1)^l \prod_{\substack{1\leq k<p\\ (\frac{k}{p})=1}} \zeta^k = -2\prod_{1\leq k\leq l} \zeta^{k^2} = -2\zeta^{\frac{l(l+1)(2l+1)}{6}} = -2\zeta^{p\frac{p^2-1}{24}}$. Now $3 \mid p^2-1$ since $p \neq 3$ ($p \equiv 3$ (4)), and $p^2 \equiv 1$ (8) since p is odd. So $3\cdot 8 = 24 \mid p^2-1$. So The constant term of q_1 is $-2\cdot 1 = -2$. But $q_1(x) = f(x) + \sqrt{p^*}g(x)$ where $f(x), g(x) \in \mathbb{Z}[x]$. So we must have $a_0 = -2$. Therefore $a_l = -a_0$. So (3.4) now yields $\sum_{k=1}^{l-1} a_k\zeta^k = \sum_{k=1}^{l-1}(-a_k)\zeta^{l-k} = \sum_{k=1}^{l-1}(-a_{l-k})\zeta^k$ (after replacing k by $l-k$), and $\{\zeta, ..., \zeta^{l-1}\}$ is a $\mathbb{Z}$-linearly independent subset. So $a_{l-k} = -a_l$ for $1 \leq k \leq l-1$, and so by the above, $a_{l-k} = -a_l$ for all $0 \leq k \leq l$. We can therefore rewrite $f(x)$ as $2(x^l-1) + b_1x(x^{l-2}-1) + b_2x^2(x^{l-4}-1) + ... + b_{\frac{l-1}{2}}x^{\frac{l-1}{2}}(x-1) = \sum_{k=0}^{\frac{l-1}{2}} b_k x^k(x^{l-2k}-1)$, $b_k \in \mathbb{Z}$ for all $0 \leq k \leq \frac{l-1}{2}$ (with $b_0 = 2$).

Replacing x by $i = \sqrt{-1}$, we see that $x^k(x^{l-2k} - 1)$ depends on whether $p \equiv 3$ or 7 (8).

Let $p \equiv 3$ (8). Then $l \equiv 1$ (4) and simple calculation yields

$$i^k(i^{l-2k} - 1) = \begin{cases} 1 - i & \text{if } k \equiv 1, 2 \ (4) \\ -(1 - i) & \text{if } k \equiv 0, 3 \ (4) \end{cases}$$

$p \equiv 7$ $(8) \Rightarrow l \equiv 3$ (4), and the same type of calculation yields

$$i^k(i^{l-2k} - 1) = \begin{cases} 1 + i & \text{if } k \equiv 3, 2 \ (4) \\ -(1 + i) & \text{if } k \equiv 0, 1 \ (4) \end{cases}$$

Writing $i^* = \begin{cases} -i & \text{if } p \equiv 3 \ (8) \\ +i & \text{if } p \equiv 7 \ (8) \end{cases}$, we see that $f(i) = \sum_{k=0}^{\frac{l-1}{2}} \pm b_k(1 + i^*) = y_2(1 + i^*)$ where $y_2 \in \mathbb{Z}$.

Now,

$$\begin{aligned} g(x) &= \frac{1}{2\sqrt{p^*}}(q_1(x) - q_{-1}(x)) \\ &= \frac{1}{\sqrt{p^*}} \left(\prod_{\substack{1 \leq k < p \\ \left(\frac{k}{p}\right) = 1}} (x - \zeta^k) - \prod_{\substack{1 \leq k < p \\ \left(\frac{k}{p}\right) = -1}} (x - \zeta^k) \right) \end{aligned}$$

And so

$$\begin{aligned} g(\zeta) &= -\frac{1}{\sqrt{p^*}} \left(\prod_{\substack{1 \leq k < p \\ \left(\frac{k}{p}\right) = 1}} (\zeta - \zeta^{-k}) \right) \\ \text{and } g(\zeta^{-1}) &= \frac{1}{\sqrt{p^*}} \left(\prod_{\substack{1 \leq k < p \\ \left(\frac{k}{p}\right) = 1}} (\zeta^{-1} - \zeta^k) \right) \end{aligned}$$

A similar line of reasoning as for $f(x)$ gives us that $g(\zeta) = +\zeta^l g(\zeta^{-1})$. Following the same steps as for $f(x)$, we find that, writing $g(x)$ as $\frac{1}{\sqrt{p^*}} \sum_{k=0}^{l} a_k x^k$, we get $a_{l-k} = +a_l$ for all $0 \leq k \leq l$ (with $a_l = a_0 = 0$ this time). We can therefore similarly rewrite $g(x)$ as $\sum_{k=0}^{\frac{l-1}{2}} b_k x^k(x^{l-2k} + 1)$, $b_k \in \mathbb{Z}$ (remembering that $g(x) \in \mathbb{Z}[x]$ by 3). A similar argument shows that $g(i) = \sum_{k=0}^{\frac{l-1}{2}} \pm b_k(1 - i^*) = \xi_2(1 - i^*)$ where $\xi_2 \in \mathbb{Z}$.

Now $l \equiv 3\ (4)$, so $q_1(i)q_{-1}(i) = 4m_p(i) = 4(1+i+...+i^l) = 4\cdot((1+i-1-i)+(1+i-1-i)+...+(1+i-1)) = 4i$

So $f(i)^2 - p^* g(i)^2 = f(i)^2 + pg(i)^2 = 4i$, and so $y_2^2(1+i^*)^2 + p\xi_2(1-i^*)^2 = 2y_2^2 i^* - 2p\xi_2^2 i^* = 4i$ or, dividing by $2i^* = \pm 2i$,

$$y_2^2 - p\xi_2^2 = \pm 2$$

$$\Rightarrow \quad (y_2 + \sqrt{p}\xi_2)^2 (y_2 - \sqrt{p}\xi_2)^2 = 4$$

Now y_2, ξ_2 are odd, else $y_2^2 - p\xi_2^2 \equiv y_2^2 + \xi_2^2 \equiv 0 \not\equiv \pm 2\ (4)$. So the coefficients of $(y_2 + \sqrt{p}\xi_2)^2 = (y_2^2 + p\xi_2^2) + 2y_2\xi_2\sqrt{p}$ are even. We can thus write $a = \frac{(y_2^2 + p\xi_2^2)}{2}, b = y_2\xi_2 \in \mathbb{Z}$ and get

$$a^2 - pb^2 = \frac{(y_2 + \sqrt{p}\xi_2)^2 (y_2 - \sqrt{p}\xi_2)^2}{2 \cdot 2} = \frac{4}{4} = 1$$

This solves the equation, where

$$(a, b) \quad = \quad \left(\frac{i^*}{4}(pg(i)^2 - f(i)^2)\ ,\ \frac{1}{2} g(i) f(i) \right)$$

where we can directly compute $f(i)$ and $g(i)$

To apply this method to the general case of Pell's Equation (where d is square-free but not necessarily prime), since d is square-free, it can be written as $d = \prod_{k=1}^{r} p_k$ where the p_k's are rational primes. So it suffices to study the case where $d = pq$ for primes p and q and deduce the general case by induction. We will not describe said case in depth here since this paper mainly focuses on prime cyclotomic fields, but we remark that taking $\mathbb{Q}(\zeta_{pq})$, $m_{pq}(x) = m_p(x) m_q(x) \frac{(x^{pq}-1)/(x-1)}{((x^p-1)/(x-1))\cdot((x^q-1)/(x-q))} = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$ which can be shown to be irreducible by a similar method as the simple proof for showing that $\sum_{k=0}^{p-1} x^k$ is the minimal polynomial of ζ_p in $\mathbb{Z}[x]$. Following the same reasoning as in the case where $d = p$, we can write $4m_{pq}(x) = f(x)^2 \pm pqg(x)^2$ where $f(x), g(x) \in \mathbb{Z}$. The rest of the problem is solved in a similar fashion as well.

Using some interesting approximation methods and quadratic number fields, Ireland & Rosen [5] show that $x^2 - dy^2 = 1$ has *infinitely many solutions* for any square-free integer

d (including $d = 2$), and that every solution has the form $\pm(x_n, y_n)$ where $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ for some solution (x_1, y_1) and $n \in \mathbb{Z}$.

Acknowledgment *Many thanks to Professor Dan Segal, All-Souls College, Oxford, for his advice.*

References

[1] Borevich, Z. I., and Shafarevich I. R., Number Theory, Academic Press, New York, 1973.

[2] C. S. Dalawat, Primary units in cyclotomic fields, *Annales des sciences mathématiques du Québec* to appear, 2011.

[3] G. L. Dirichlet, Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires, *Journal für die reine und angewandte Mathematik* 17, pp. 286-290, 1837.

[4] V. Flynn, *Algebraic Number Theory Lecture Notes*. University of Oxford. Oxford Mathematical Institute, Oxford, UK. 2011. Lecture Notes.

[5] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1982.

[6] S. Lang, Algebraic Number Theory, Springer-Verlag, New York, 1986.

[7] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.